ID: 404084
Cookbook: browseurl.jbs
Time: 17:38:58
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report https://goldberglaws.com/ 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Phishing: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 9
Public 9
Private 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 40
No static file info 40
Network Behavior 40
Network Port Distribution 40
TCP Packets 41
UDP Packets 42
DNS Queries 44
DNS Answers 44
Code Manipulations 44
Statistics 45
Behavior 45
System Behavior 45
Analysis Process: chrome.exe PID: 4136 Parent PID: 5112 45
General 45

File Activities 45
Registry Activities 45
Key Value Modified 45
Analysis Process: chrome.exe PID: 4676 Parent PID: 4136 46
General 46
File Activities 46
Registry Activities 46
Disassembly 46

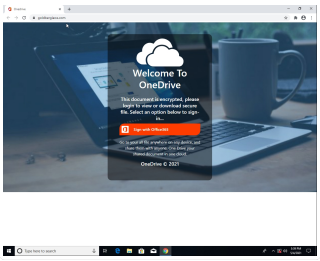
Analysis Report https://goldberglaws.com/

Overview

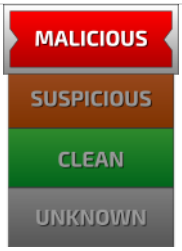
General Information

Sample URL:	http://https://goldberglaws.com/
Analysis ID:	404084
Infos:	

Most interesting Screenshot:



Detection



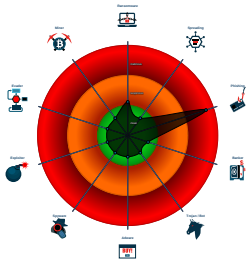
HTMLPhisher

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish7
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 4136 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://goldberglaws.com/' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4676 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1572,3517170012200295616,8387480202046539603,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1812 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

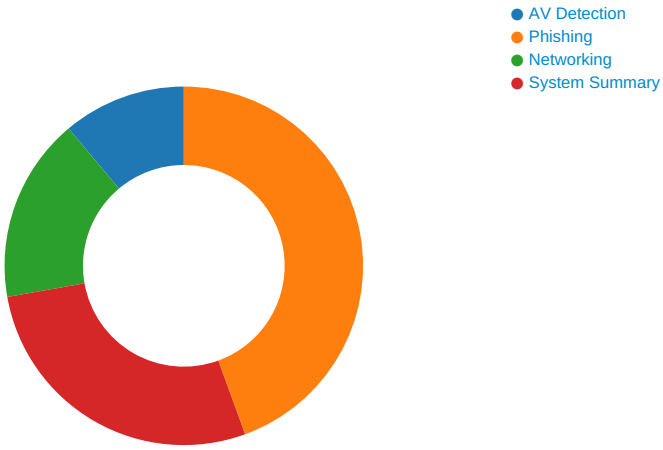
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

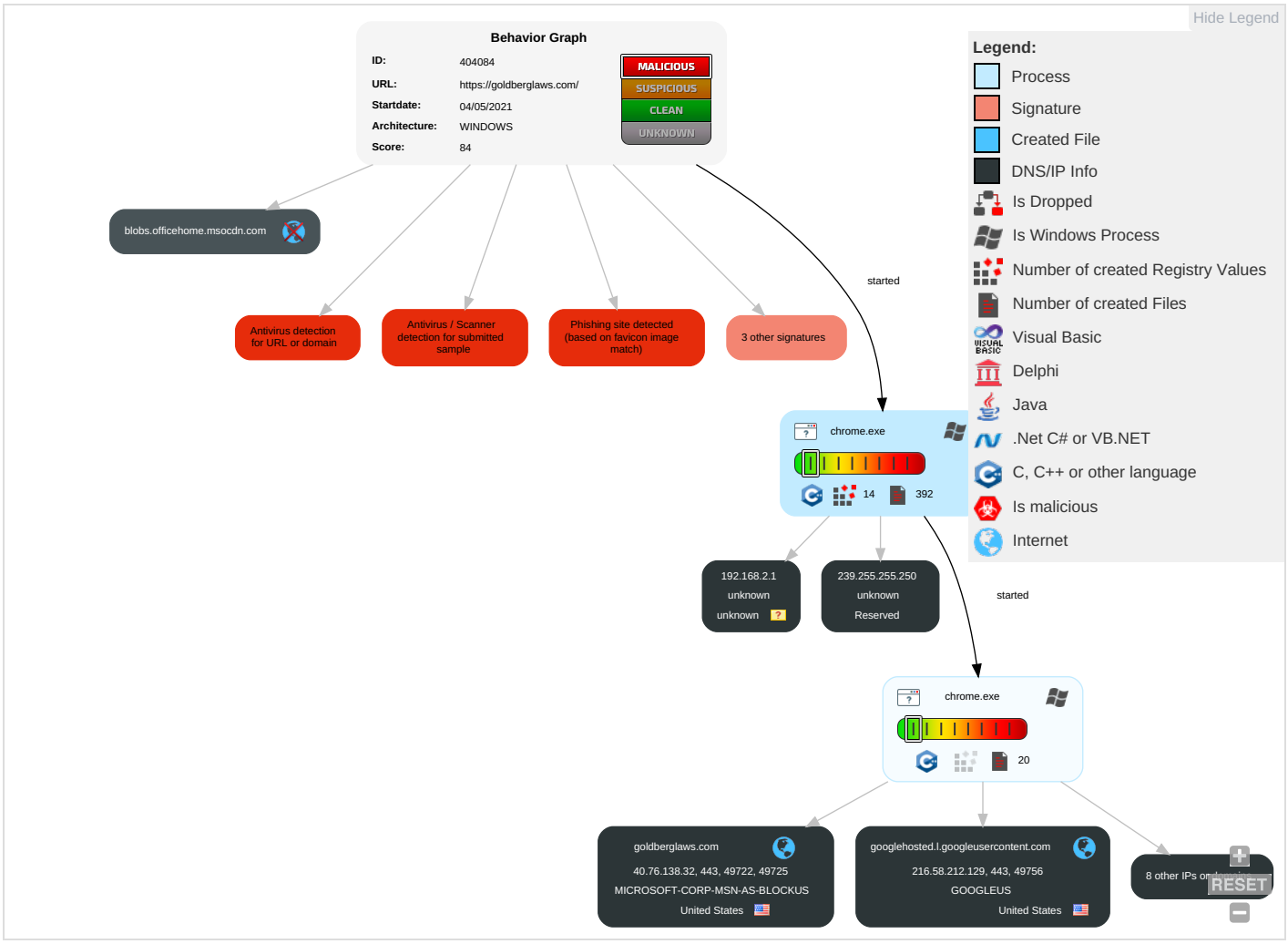
Yara detected HtmlPhish7

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitior
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

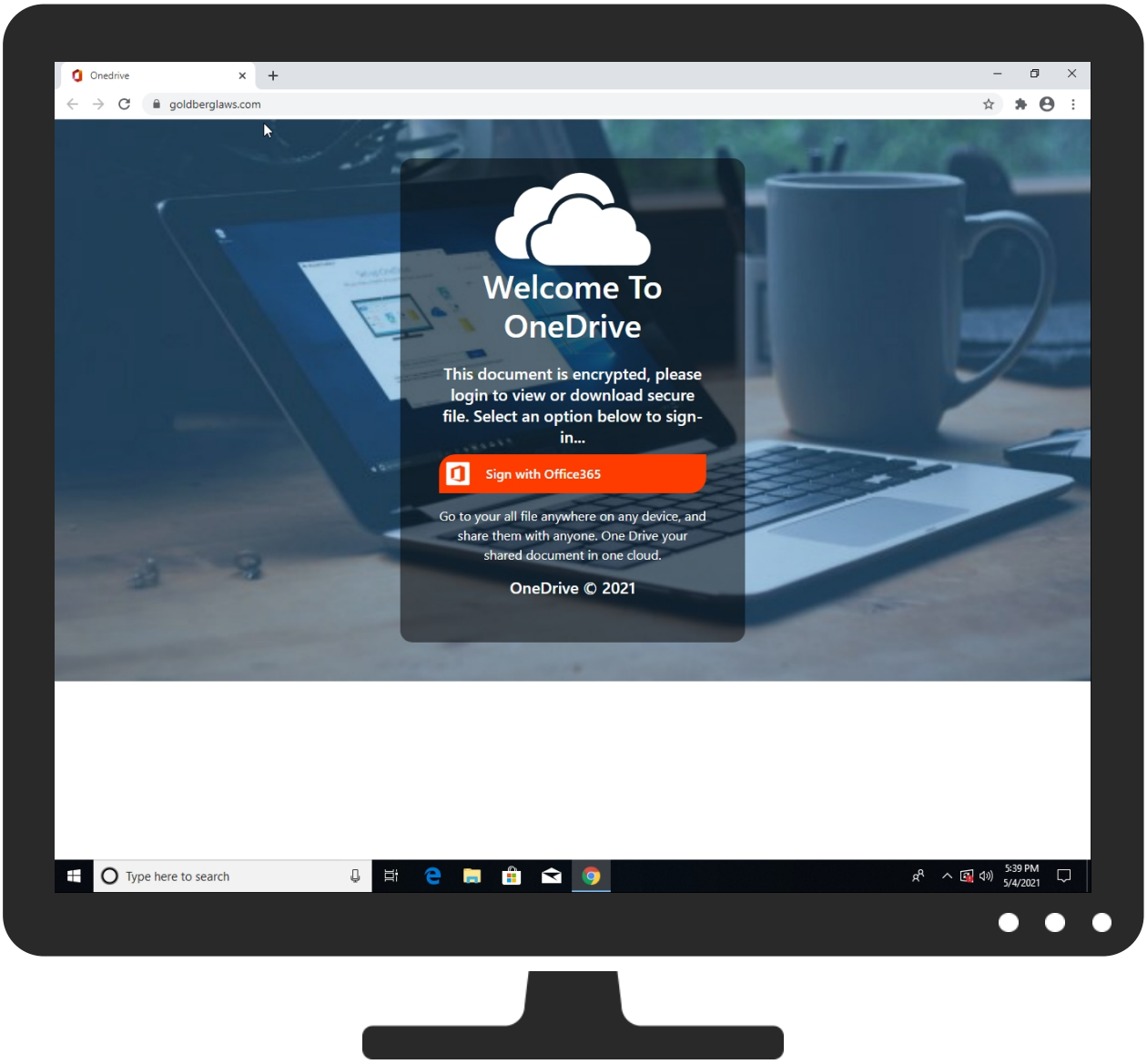
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://goldberglaws.com/	2%	Virustotal		Browse
http://https://goldberglaws.com/	100%	Avira URL Cloud	phishing	
http://https://goldberglaws.com/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://goldberglaws.com/-J	100%	Avira URL Cloud	phishing	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://goldberglaws.com/2	100%	Avira URL Cloud	phishing	
http://https://blobs.officehome.msocdn.com/images/content/images/favicon-8f211ea639.ico	0%	Avira URL Cloud	safe	
http://https://goldberglaws.com//	100%	Avira URL Cloud	phishing	
http://https://goldberglaws.com/Onedrive/	100%	Avira URL Cloud	phishing	
http://https://goldberglaws.com/Onedrive	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdnjs.cloudflare.com	104.16.19.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
googlehosted.l.googleusercontent.com	216.58.212.129	true	false		high
goldberglaws.com	40.76.138.32	true	false		unknown
blobs.officehome.msocdn.com	unknown	unknown	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
ka-f.fontawesome.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high

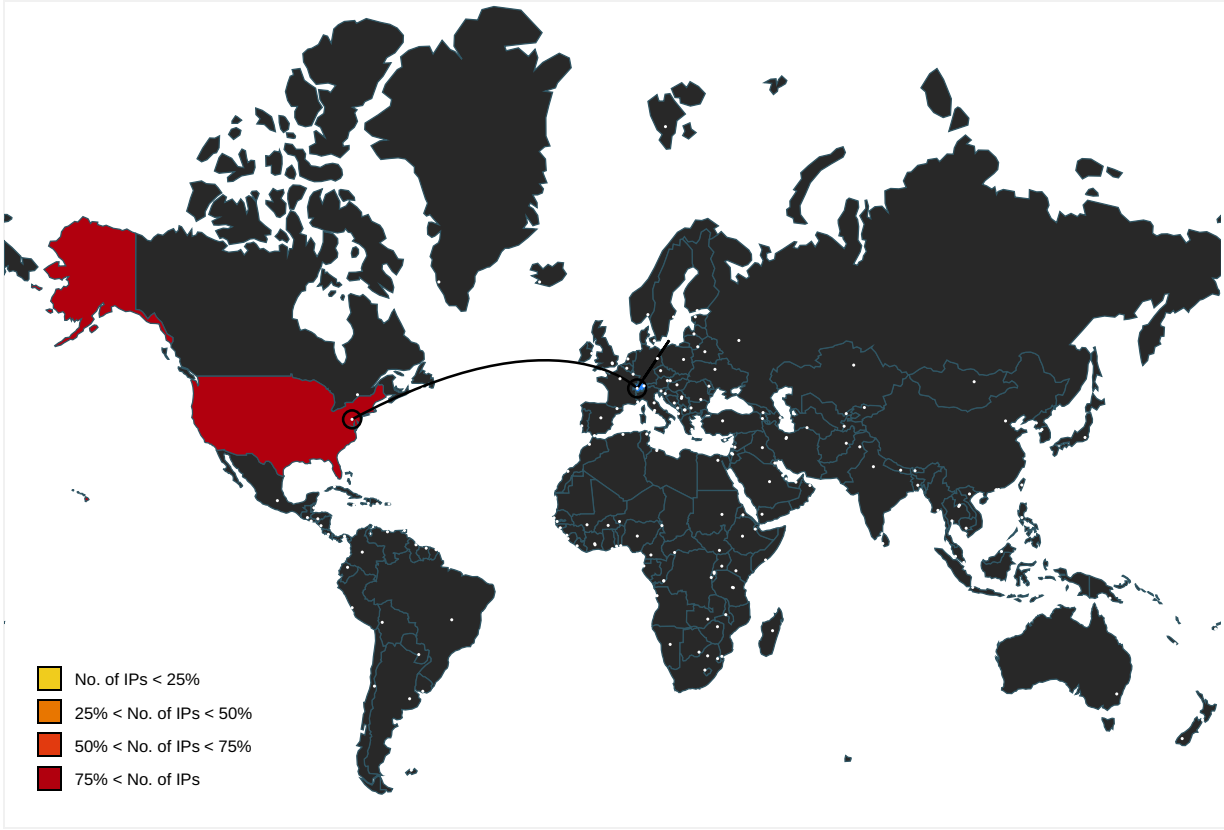
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://goldberglaws.com/	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://goldberglaws.com/-J	adbf4030bbd380bd_0.0.dr	true	• Avira URL Cloud: phishing	unknown
http://https://dns.google	97b4f9d4-bab1-4664-9472-59383c235807.tmp.1.dr, 4da3fdb6-b569-4210-a000-d856e2a3030b.tmp.1.dr, 38bff282-14fe-4d23-a7e5-280bc3a6d216.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://a.nel.cloudflare.com/report?s=Qrt2Y3oUEU%2FA9jZUuyWr3QXfeBHWUn70Lrdf%2Fc51aXQ1hUfivhVgvU5Ct7	Reporting and NEL.1.dr	false		high
http://https://a.nel.cloudflare.com/report?s=aYNOt6dCbXuhZWlT6ppdhfwZ53Hbt%2F%2FF5toC4n0qRpWhxIwyY%2F%2B6%2	Reporting and NEL.1.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js	b2520ccc0a0a3903_0.0.dr	false		high
http://https://goldberglaws.com/2	History Provider Cache.0.dr	true	• Avira URL Cloud: phishing	unknown
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	47388fd446fbc78a_0.0.dr	false		high
http://https://blobs.officehome.msocdn.com/images/content/images/favicon-8f211ea639.ico	Favicons.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://code.jquery.com/jquery-3.1.1.min.js	adbf4030bbd380bd_0.0.dr	false		high
http://https://goldberglaws.com//	4fec2c7937dd26f8_0.0.dr	true	• Avira URL Cloud: phishing	unknown
http://https://clients2.googleusercontent.com	4da3fdb6-b569-4210-a000-d856e2a3030b.tmp.1.dr	false		high
http://https://kit.fontawesome.com/585b051251.js	7bc2a1ab566f2cf6_0.0.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	4fec2c7937dd26f8_0.0.dr	false		high
http://https://goldberglaws.com/Onedrive/	History.0.dr	true	• Avira URL Cloud: phishing	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://goldberglaws.com/Onedrive	History.0.dr	true	• Avira URL Cloud: phishing	unknown
http://https://goldberglaws.com/	7bc2a1ab566f2cf6_0.0.dr, Favicons.0.dr	true		unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.212.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
40.76.138.32	goldberglaws.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404084
Start date:	04.05.2021
Start time:	17:38:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://goldberglaws.com/
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	2

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.phis.win@28/174@9/7
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 40.88.32.150, 52.255.188.83, 216.58.212.173, 142.250.185.78, 142.250.184.195, 142.250.185.206, 69.16.175.42, 69.16.175.10, 142.250.186.170, 142.250.184.234, 104.18.23.52, 104.18.22.52, 95.168.222.141, 8.238.85.254, 8.241.89.126, 8.241.89.254, 8.241.78.254, 8.241.90.254, 142.250.185.67, 172.64.101.17, 172.64.100.17, 142.250.185.138, 184.30.25.140, 142.250.185.170, 142.250.185.202, 142.250.185.234, 142.250.181.234, 216.58.212.170, 142.250.74.202, 142.250.186.42, 142.250.186.74, 142.250.186.106, 142.250.186.138, 142.250.184.202, 172.217.18.106, 172.217.23.106, 93.184.221.240 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, cds.s5x3j6q5.hwcdn.net, ka-f.fontawesome.com.cdn.cloudflare.net, r2---sn-n02xgoxufvg3-2gbs.gvt1.com, clientservices.googleapis.com, wu.azureedge.net, skypedataprdcoleus15.cloudapp.net, clients2.google.com, e12520.g.akamaiedge.net, redirector.gvt1.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, kit.fontawesome.com.cdn.cloudflare.net, fonts.googleapis.com, accounts.google.com, content-autofill.googleapis.com, ajax.googleapis.com, fonts.gstatic.com, wu.ec.azureedge.net, ctldl.windowsupdate.com, www.googleapis.com, skypedataprdcoleus17.cloudapp.net, r2.sn-n02xgoxufvg3-2gbs.gvt1.com, blobcollector.events.data.trafficmanager.net, wildcard.officehome.msocdn.com.edgekey.net, clients.l.google.com • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:39:48	API Interceptor	2x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	117192
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	3072:F2qSSwIm1m/QEBbgb1om2qSSwIm1m/QEBbgb1oQ:FJdwIm1m/QEOb1omJdwIm1m/QEOb1oQ
MD5:	2FEBC5EB397A71B7A4862D0DCC21CA5E
SHA1:	5568FBD6D7DB899850D3AAFF95FEC08952361678
SHA-256:	2E9BE05B763D01CB0CD6FDE8BC64432A012AD3ECD9A6F3099DDE740A2D148A13
SHA-512:	B7D42B634F3B0CDC81CB94F281C8BB743BB98421AE54E21005637F762292D865EB1D71D43C4FF96AEE824527E9F7FB94FE5F5A4D35A22363A2A86AF8ABE0C414
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-J...."Y...$E.KB..D...D.....3.n..u.....\|..=H4..c&.....f.,..=..-....p2.:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s..,.f`D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.12395863637513
Encrypted:	false
SSDEEP:	12:SwTJrkPlE99SNxAhUe0hicwTJrkPlE99SNxAhUe0ht:15kPcUQUPhiT5kPcUQUPht
MD5:	045303D5FD10A119422476D931DBE46D
SHA1:	F996DE905E695D3873A990601522FC9A9B480150
SHA-256:	E9F087E813BCBEBEC557099264D3D73F319629C132BD2ABF3F105125B5C9E99D
SHA-512:	1CD236A55BDB524B2D9423EF4D81042D136AF42E5AB058DDBEB4F2EAEF299292CA7F3DB484E35BB87F8A72D474F7D848F3DB488D269FE81565007F161E86E0EF
Malicious:	false
Reputation:	low
Preview:	p..... .....a.7..@..(..... .....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...p..... .....M0..@..(..... .....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\0a2061d3-756a-4398-8901-a5899948f04e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	168434
Entropy (8bit):	6.081103024937884
Encrypted:	false
SSDEEP:	3072:eS7i8A6zsByu8VXAVzkbOBLvMlNEopvR/XQrXaFcbXafIB0u1GOJmA3iuRG:T7T7OoQVzkq9vMwSR/LaqfIlUOoSiuRG
MD5:	523915877C9D9F6DCB1071823A646418
SHA1:	1F4671A4C526F047B9C6F711A813B540BBF8B52F
SHA-256:	EBEB5102028767336EC8F9D6077676BE4F2E42832CB43445F620208DE86DD1B3
SHA-512:	04D68EB74FDE045E55EA7512F76A5F1DEAEEE892330E670D5658DBDAE5B005984907E0CCAA3B9AC403D42F8D8D1A65EDCB7C2639C2E84D27EC48D84190DB853
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620142786669139e+12,"network":1.620142788e+12,"ticks":303096093.0,"uncertainty":3464151.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715095491"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\70f4e063-4855-4491-8150-455cca753904.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92068
Entropy (8bit):	3.748868790444244
Encrypted:	false
SSDEEP:	384:vLIX3taUNlKb2Njrov/l34HtUH9UGkTrOJDPx4559YrSfmKtKVrLLUOBJDN21jS4:cK1FiRE0Meb/xBQH/+9KPVrYv
MD5:	297AF78D086A2D396D6D4EDEBACB6109
SHA1:	1AF86A93CB4B164CB37461AFF1A3F0C260E5F244
SHA-256:	CF558829070BAB26AA7EADFC4D2A0698067A70AB6963654D48E402A28CF8FB14
SHA-512:	5F5F10CB9E275E3C3285679A9F2A02CB79F64AF49A2F4C3643C35576BD76BA3649BE84D4A526EE978AC63A95BB0205B47DABA5EB832FC6DCBD322AC87029B82
Malicious:	false
Reputation:	low
Preview:	.g.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....98.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\79002b7b-0872-4a71-8d4c-6d26cfcd773d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	168434
Entropy (8bit):	6.081102345440459
Encrypted:	false
SSDEEP:	3072:IS7i8A6zsByu8VXAVzkbOBLvMlNEopvR/XQrXaFcbXafIB0u1GOJmA3iuRG:Z7T7OoQVzkq9vMwSR/LaqfIlUOoSiuRG
MD5:	C829B190EA3B5D3C28516E7BCBACF0BD
SHA1:	D72FD34A1FC185812300DBB237FB0762CA37E2AE
SHA-256:	8DDEEE2121E5C3FB62C38EF924B4BDF715D131DB200126E7B8617D1216C3348C
SHA-512:	473FD47E4CBD1F2DE345915C8F78EA2691D00278991DCCA7C10C360C9A8CF79BBE3CC5220CF3FCF35DAEAEFA80B6113A5CC4C6E3B8FD14807D5E4C614F0A8DF5
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620142786669139e+12,"network":1.620142788e+12,"ticks":303096093.0,"uncertainty":3464151.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C59
Malicious:	false
Reputation:	low
Preview:	sdPC....................UO..E.D.Q.o....sdPC....................UO..E.D.Q.o....sdPC....................UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0c9dbef5-8f6b-47c8-878e-512fb9a7b7f9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1541
Entropy (8bit):	5.580138665999726
Encrypted:	false
SSDEEP:	48:Y9gVwUk6UUhRNeUCKKUVqPeUekUebNzwUfO1sYU2nUeP:MUdUU3gUCKKUAPeU3UMyUW2YU2nUg
MD5:	D9DF2C2841EC2EAEF1371C90371FAEAF
SHA1:	D28AF2A7D515FFAF71CCF9FA4507B7CBA31F323D
SHA-256:	1E55D45AA0438A5F2E7903233DC5088B567B02E9EAAAD45FAC0F5DC877D73F0B
SHA-512:	4567BDBBD769278BCDD858F4C74942A7BFA41EFA1B7699240A78E25B79D3B557F132CCAA60536E00E960329BE580FA74F2C258CEB186A243B79F1CA9665D2F0D
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1635922788.784387,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620142788.78439},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1651678788.464625,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXIu9G3fM8KGQt4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620142788.46463},{"expiry":1651678788.44738,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620142788.447384},{"expiry":1632987007.31909,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601451007.319093},{"expiry":1632987013.78633,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\29a25dad-a957-4f03-a9fb-156f95fb8da4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5714
Entropy (8bit):	5.166821449628878
Encrypted:	false
SSDEEP:	96:n/LphfUaybyIV1N5k0JCKL89ak891d5bOTlVuHn:n/XfUbyIlh4KDk89zv
MD5:	2DFEA5D310EFE55F6B64BAC16E8020AD
SHA1:	A367B0550CDD6E114329DFC3B9B9AD7E69784A1C
SHA-256:	0AF0CF8FFB0C3F0DC9EFECA945847760D28319972BE0E0C9023F4E650AD1A073
SHA-512:	C2F7240A689DB4C2E5B723F1CEA11CF31570B492B6B44BA6EC4A32C81F27CDD9E5055337129F998C9EEEAD47E67BA1CA5CA7D95806AFC7FA4FE96030F3718FB
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264616384406410","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4da3fdb6-b569-4210-a000-d856e2a3030b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3473

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4da3fdb6-b569-4210-a000-d856e2a3030b.tmp	
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4f757f7c-4656-43a0-9a31-979c7d6c4430.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5118
Entropy (8bit):	4.960862545703114
Encrypted:	false
SSDEEP:	96:n/LLhfpIV1N5k0JCKL89ak891d5bOTlVuHn:n/JfpIlh4KDk89zv
MD5:	92DA909979D89D78843ADF54EC118827
SHA1:	C74B7DB1EC63BD4CA14D0EBE931183C6D219406F
SHA-256:	AC3D22A0D39D8D8BDDB0151E14FF3219BC9156322EF278A7D633C7B328C8C719
SHA-512:	6BBA8A21288A47682FB711EECC31AF66F863A7933E000294CD5F7A15F09C292C0020916A88D38E1685EE61E7114F27652EBDAF83E2649902B65BE186F06D6117
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264616384406410","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7ff1257a-4640-417f-9b9b-fc2d4042f0e0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9dd22213-a0ee-4249-b435-d6b3632e2d73.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22601
Entropy (8bit):	5.5364191017687725
Encrypted:	false
SSDEEP:	384:DNGt2LlgsXN1kXqKf/pUZNCgVLH2HfD/rUqqHGInZpywAj4d:nLlzN1kXqKf/pUZNCgVLH2Hf7rUzGInh
MD5:	FA706363382A7F32A9E3E9727E1C185B
SHA1:	425BC0E6E8E526AE46F7138165BB7122D499FB1C
SHA-256:	FD423BA12AD924462E4EF9C90159AE6CC22C5D1029794191BB934C4EC4A2ED0C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9dd22213-a0ee-4249-b435-d6b3632e2d73.tmp	
SHA-512:	61B8DB864BE3A228AA970B4FCDB21DFEE3D3E5C8CE43ECD772D80EB4407C0F1C27B890C1A94877D4499D850BE17437A5845D09BDDC2660FBDB4F59EC9414979
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13264616384083393","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.24256802186893
Encrypted:	false
SSDEEP:	6:msFHNq2Pwkn23iKKdK9RXXTZIFUtpdFZUZZmwPdFgkwOwkn23iKKdK9RXX5LJ:tFHNvYf5Kk7XT2FUtpdFu/PdFg5Jf5KU
MD5:	4964A8C38ACE4F3A4208C86F2FEBA24E
SHA1:	8EAF40996CC47DA11ABD715399B2DB7DB560CEC9
SHA-256:	BF1058BF0A71578E1431A25569B5E69E0EB2D3ABC13DE4CD7DEAF82B7089E318
SHA-512:	0A237B57E4E8077CC6B22047E588BC67302698691AB39C4456CB8571A26AB753EC76613F5861B9D195B2328DDE9DB02EBC1638DD130C77232600B201741BC593
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:39:54.592 17a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/05/04-17:39:54.598 17a0 Recovering log #3.2021/05/04-17:39:54.602 17a0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.242142467778228
Encrypted:	false
SSDEEP:	6:msF0FIq2Pwkn23iKKdKyDZIFUtpdFSZZmwPdFpkwOwkn23iKKdKyJLJ:tF0FIvYf5Kk02FUtpdFSZ/PdFp5Jf5K1
MD5:	12FB7644F5455A78160F7C984B79C1B9
SHA1:	EBB650AF46FDEB3AF1E952B7B74AE977CD449A3E
SHA-256:	04DB9A8D52FD99676F97D5A43845BB82AC5707B35FCA21A9AF4D707DD0E8787F
SHA-512:	FF5096C768BAB4D0AE30E3A2929C9EA157C5D01153B6FE16000A21630AE7F1CA23B878926D26293702AC94F0375E4B95ACBE2CF8258ACA6F68FBB9A800850641
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:39:54.563 17a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/05/04-17:39:54.583 17a0 Recovering log #3.2021/05/04-17:39:54.584 17a0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\47388fd446fbc78a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.499310388376117
Encrypted:	false
SSDEEP:	3:m+lya/l08RzYP2FycyGYWCULLuFvDA/A6ElZ3ZElflHCmOzltfu/q6910NhP5mJM:m1GYerCUQWlAt+97Gt4JSK6t
MD5:	8E75CC64FA2FDB375B9901ABCB79733C
SHA1:	117AA1DCBFFC85059CA7B7C3E052DD86964C2BEC
SHA-256:	A8267BF968C3796719C180FF317829EB2EE3063CE9C6306B32F1DC7C3C40EC7C
SHA-512:	19C18A3A5C285BA7AA769C282039591EA6D6F9B24A5A3ED8ACDF7903ED2E83354D5FD2C6307EAA90C462BA3F7D8280E1F75A36E18DADD0F1ED09988D65FB5092
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...-tGV...._keyhttps://code.jquery.com/jquery-3.2.1.slim.min.js .https://goldberglaws.com/.=.+. /.....:U..C/(+5oW}VV..Sl7.?z.Xy....y.A..Eo.....WL.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4fec2c7937dd26f8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.437839244630676
Encrypted:	false
SSDEEP:	6:maY68E9xEEUgLEroiohWqc5E5prDkK6t:9YgvnWz5E5pO
MD5:	9F83116175D40AAAC0019EE84CDAE3A7
SHA1:	FFE33FB483D56520E66C6379032AC4D6B8747B46
SHA-256:	A999BD40E77A474ED71C23ED8C988018EA7A048B2CB67E0D5570FD403E5A94C7
SHA-512:	5EEA9F8BAC9FDA5ACC67A080125E80CB9E08CE4DC42903994B82C4F26432E8AD3E7046C46595D4707BCC887AF8CE4386499044FAC3B07E537F0BD3F5CAF6E9 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b....W|a...._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js .https://goldberglaws.com//..+. /.....{...S.....J.....Cn.Z..z6.A..Eo.....M0Y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7bc2a1ab566f2cf6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.482399621732888
Encrypted:	false
SSDEEP:	6:maYlNYpSVk5kJKv6eZ5yjjugppLrjZK6t:ZpSV4kEvhZsjigppv
MD5:	FC7F4E6E0F67F9EB85927AB072C36580
SHA1:	ECBF006F40D7C8112D6AA6652CB509DDD4D2670F
SHA-256:	3EB70D41767E87ED82C1FA8CDE3E08284521AA0A7389FE7AD2DAC1D471D28EE8
SHA-512:	FA0D7F9FD4FC25DA081A508064DEC8DF0283A8556709A91CF6FCAF3F49E5326C144870D23B214E01E6DB10B3019B9F46DD6D1C8C1E7889F78BD051B98322470
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...KNnF...._keyhttps://kit.fontawesome.com/585b051251.js .https://goldberglaws.com/...+. /.....b.....d..,22.....o.vZ$..6Fj.V..0Z..jt.A..Eo.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a5405809f683b2b0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.492685572557809
Encrypted:	false
SSDEEP:	3:m+l1HWgOA8RzYRhmHT8NWQABKidFvDA/A6ElZ3gzclHCnlx58+Ecn6VyT9kg4mw3:mYHOYSHT8NWQA8IoLntLzxkgr0nK6t
MD5:	57B2F3DA2B05C754013326382EC034C1
SHA1:	EC7E1D36A7C2CC3E67798ADA85C4A5A75F65CC5C
SHA-256:	1FBD469A021CECB82942FA113348A97EE7B2586AB538D559A75751941A7FA1A0
SHA-512:	29918FD294BF3F1DFAC4DB77BFA742446500AB23863E7FC3CC016D0D722F433D0E9709206B909009228E66A78055C7991D7184262523E6140D4AF05D0D33236E
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...IA.g...._keyhttps://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js .https://goldberglaws.com/.`.+. /.....k5.l."....M(.k9..dL...tRWi...A..Eo.....L .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\adbf4030bbd380bd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	206
Entropy (8bit):	5.518221976413484
Encrypted:	false
SSDEEP:	3:m+lOGXllla8RzYP2FycyG8ZFvDA/A6ElZ3hJelHC6JtqGMkCiRwpdPL2OG44mV5:me1/VYeMzJJ16JYGMiRwzzoYV3hK6t
MD5:	B2FF148CB434984C6EDFA923399D39A7
SHA1:	09144CB9E906A20814E27D07FF2AFFC111A32A5B
SHA-256:	DA21EC33AA364FAAE00C642A7DBF8F735DDCCB62DDA8853B3EA090325A8B96BE
SHA-512:	5D5D3585256104ACCED6D9682A8A4A8F729DF2C6734F090E8357DCAB07FD6323E114F4BB38021FA7A3DA19C50590D2D7579E216AB38421C4578126BDEEA4E96

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\adbf4030bbd380bd_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J....._keyhttps://code.jquery.com/jquery-3.1.1.min.js .https://goldberglaws.com/-J.+. /.....U.....ib5....].V3....;.....[...RI..+.A..Eo.....ea.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b2520ccc0a0a3903_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.520390681060061
Encrypted:	false
SSDEEP:	6:mCIEYET08NaYWbVOqZob16ptC8p9C44n7DK6t:rg8NaY8ZobON9C4e1
MD5:	019A64F91C614660167DD6E90F1C310E
SHA1:	851649BA6412081084DA570AAD54038E554D97EC
SHA-256:	A2FB41779F8368178A451E866678A35F47C800A1282475FB16C427D6AE722C00
SHA-512:	9DAFF664AF7D38A9CF3E7DA656645585EAB7F8DD702F81E36F602A839C25B2C4D558FEBFCF179309A873FED990002C095963FE59C9BC7ECBC81ADE6A5D6BA3 6F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....P>...._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://goldberglaws.com/.n.+. /.....M.i.....J..mo.-5...ji"....A..E o.....~9.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d500866a31b827d9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.5607124424934815
Encrypted:	false
SSDEEP:	6:mYQXYSHT8NWQAlKPUQyrrHZKvsU6P4vWjbK6t:FKz8NWQCUUNdKvs5PyW5
MD5:	A1FB13F08522BFB0F0530DF3A2666BA3
SHA1:	C722963C9577A4DA3B3C803567EDBA4F633FA16E
SHA-256:	72E844380EE4D166C87891BE1012ECD056A7B118ABFA512AC1AF2904F48AFED7
SHA-512:	088309383EDE5CE4EB5C3DF083E3B4B2D09501EEE62601354E613242D2B1C93EF87ED6212A8152B1AED1926A177CB55298E84B606B1293351025332956C76B50
Malicious:	false
Reputation:	low
Preview:	0\r..m....._.....=N...._keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js .https://goldberglaws.com/...+. /.....Z.....3."0.....v,1c.I*O..u..9..|..i.U.A..Eo..... ..zsR.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	408
Entropy (8bit):	4.975036621182953
Encrypted:	false
SSDEEP:	6:mdl28XOO8/O6bcFq2LcTxzPawAfyDnzQn:al2H/rFZXUyXQn
MD5:	2423E82CA3A2391B201C9EA4C5DC2E0E
SHA1:	AE303E020AEC8711A379B4E5A56893EBA72E6EE1
SHA-256:	5BC6B3B75CD6A1A92E894BCFF55F9794DBDAE8B101E3D37071600975DE2B2089
SHA-512:	505EEA5D510AB6EBABAD7DD8592D272C8A59D70FED43F8F467CE7A0270464ABE7B19C556563B65EB0FCBECD9B2411599AC2846843DE542264A22C0756B3B4C 91
Malicious:	false
Reputation:	low
Preview:	.....Eoy retne.....X@.@..+. /.....&.7y,.O@..+. /.....9....R.@..+. /.....F.8G@..+. /.....,oV...{@..+. /.....0@..@..+. /.....'.1j....y.+. /.....^}. Np....4&../.....-..0..x..4&../...../...3...&../.....I....uW....&../.....Q.i....&../.....6,2.+.g...&../.....D....3...&../.....4T/f.C3....&../.....f_.+. /.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Entropy (8bit):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9738338009745322
Encrypted:	false
SSDEEP:	24:8Xe9H6pf1H1oNKvqLbJLbXaFpEO5bNmISHn06UwS8:8XbfvoNKq5LLOpEO5J/Kn7Ud8
MD5:	7D1AEA7B3F599FF252704825596E7810
SHA1:	D3775E478F458D77DF3E5F6907434E4DC2521A48
SHA-256:	F0734E69488E22DF2067AED126A79A7651064B4D8E92AF4C1E4EF0E09D213B2A
SHA-512:	D3A39491887183DABE5CC3F10A86EBE6DBEDF160C0841EB7596292F4298472BCEA491BDD47EDC58C9D4D03FA0137C74B081FCAD5E1EB32773E5C769260C22C10
Malicious:	false
Reputation:	low
Preview:	.....=.k..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1299
Entropy (8bit):	3.0588746417329773
Encrypted:	false
SSDEEP:	12:3olydJhTDM7w6PlpxlpNVOro6wlz3B7yMgvE/LZMIS6jlzlelpsc6w9xlpl:34SNMBlrlJf6KBdZL3S6jb656yxlL
MD5:	525411A73BB4678539D5101D504082E0
SHA1:	DCA1DFF2547AA5610F6378453B86FBA2FFCAB130
SHA-256:	EF11A8C8E288D257FC241D7C92D7652B53EFA982E6866448F9D2F90B7E1A7417
SHA-512:	8E4DF1F5FB78A0E49692BAFA0A19EBF0FB4568A10F6C06ECDB0BA911DA6DA641AAB86E21C7E1E1C7CBC7C0C97229461C8F0B9EBF1DE6D8FF7B4CCE2A27E26785
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...03584b7f_1ac3_409e_b5e5_bae66f5267f7..... .....5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....https://goldberglaws.com/.....O.n.e.d.r.i.v.e..... .....h.....`..... ..... .....~-]....-]....`.....x.....:.....h.t.t.p.s.:././.g.o.l.d.b.e.r.g.l.a.w.s...c.o.m./.....8.....0..... .....8.....h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .....=.&.....2..... .[.e.m.a.i.l. .p.a.s.s.w.o.r.d. .]. .#.0..... .....1.....e.m.a.i.l.....e.m.a.i.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
Malicious:	false
Reputation:	low
Preview:	.f.5................i.Wd...............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F..................F................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.208810918866368
Encrypted:	false
SSDEEP:	6:msy9+q2Pwkn23iKKdK8aPrqIFUtpdYEJZmwPdgCE9VkwOwkn23iKKdK8amLJ:tM+vYf5KkL3FUtpdYm/Pd9iV5Jf5KkQJ
MD5:	C7547A86FDD5354D93E07E1D1DAC07AF
SHA1:	7752652686C2B02A49A42326E9035FAA43190525
SHA-256:	9F666E36581F889BE0E6ED5593BCA6BD7F39FD5C6A0F3D38BA4A6324FD812FDE
SHA-512:	000CA6623745312B1C0EDC0492A129D57F87044AD8EE44688AC627E919581E8F23D05A6A9927CD7254D9822853ECF245144F9DC9D57AF671779AF2430476EB67
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:39:44.399 152c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/05/04-17:39:44.400 152c Recovering log #3.2021/05/04-17:39:44.401 152c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5................f.5..............f.5................f.5................f.5...............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.251042755061905
Encrypted:	false
SSDEEP:	6:ms1FN+q2Pwkn23iKKdK8NIFUtpdZmWZmwPdZNVkwOwkn23iKKdK8+eLJ:t13+vYf5KkpFUtpdkW/PdTV5Jf5KkqJ
MD5:	E4D7B0763B96BDCC0D7B6C40659C9AFC
SHA1:	EEC29099B75E760D13B3C16C96CFE14A56684A34
SHA-256:	8A3257DA8DBC14E80D17273FCB1DCFD5E670BAB093DACDB60036706201D15E8C
SHA-512:	213782C9C9140BB5D89D3D241D3642E3D7400D0A575135142F69F7ECDD9533BB8D25032E3C3E7D5C3945DDFDCB2459CAC0ED461B9249C008D3213A92829B97(
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:39:46.534 12cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/05/04-17:39:46.536 12cc Recovering log #3.2021/05/04-17:39:46.536 12cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXltmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","hqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Size (bytes):	16384
Entropy (8bit):	1.9333726561494713
Encrypted:	false
SSDEEP:	48:tBmw6fUnNPF7C4XPSR3DjmXy2rr1enMhjOO0cIa:tBCsFCoCjmXrr13D0w
MD5:	7CB0CE02A739E56A436200B3B7A640D6
SHA1:	5DD14852E364BCDEE5A83614A511ED532B58FEE9
SHA-256:	28ACF0A776256B7524FB15AB24CBBEDC515D457290CEC3D770441CE8AB6ECCCA
SHA-512:	D1A2FBE500FE75D96DE28A14B64AB6BBBD323090BEB6121240291D4F28644A1462A7B82EAF26500DCDC3E9578F3D107F07E77577F2385FA6548765D338443783
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.8142360721748629
Encrypted:	false
SSDEEP:	24:hZmwnlqLQ6kyLjtVxh0GY/l1rWR1PmCx9fZjsBX+T6Uwkt3n:S+aeCBmw6fUHt3n
MD5:	8C1D3BAE4EC0127B358141DD09395E37
SHA1:	591C8C4EA5C8712CAC5F466ACB5F2E32640726E2
SHA-256:	0799F2BD4CB59612A758BF4EA5D1E59A1C42F41CB48824379CF34DAD811F627C
SHA-512:	A4CCD277F06CE68BD48C3200DBE061CEE55F90B2B2549E61F7999E224EB76D2E61557A4F2FAE634C8861954B5D50406546E79C15CF3518069ED4EC3B0BCFC9
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.256694470094506
Encrypted:	false
SSDEEP:	6:msFhNq2Pwkn23iKKdK25+Xqx8chI+IFUtpdFAhZmwPdFVkwOwkn23iKKdK25+Xqp:tFhNvYf5KkTXfchI3FUtpdFAh/PdFV5S
MD5:	3D94C823836AA2B98D8BE0A455874B54
SHA1:	522099E30AF8D0AD4A4D0AE3D40F7FD0E4398458
SHA-256:	0C5850E1D228D3B79448A5E3816D99157501531E3CB8A2BEFEA5FF76990BCE14
SHA-512:	8C5FF37358DC4D9C8972AA945337BFEE71AAD07BB77ACF12FA0453F4FD503953CA660FB609B57F6E096FCE73448A557F8629EDD421BBA7877E643F8C40A2A5F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Preview:	2021/05/04-17:39:54.532 17a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/05/04-17:39:54.534 17a0 Recovering log #3.2021/05/04-17:39:54.539 17a0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.209568201618464
Encrypted:	false
SSDEEP:	6:msFfq2Pwkn23iKKdK25+XuoIFUtpdFuRZmwPdFkLwkwOwkn23iKKdK25+XuxWLJ:tFfvYf5KkTXYFUtpdFuR/PdFQw5Jf5Ky
MD5:	6EEB6FC904FE92D34EE802CCBFC33C2E
SHA1:	B88ED77CE03FB4F72E0A0DE7EC243C8113E32030
SHA-256:	AC5A68937B3CF54F57E736BFEA56A08868A38ECC1B6CFFBCDF2A20E54522B5DE
SHA-512:	CF7C232896F3CD2CB4AA63473CA1D4D94C475664D70467826D7CF700AB8A888014E76BEB7D131D05D6F3FE5543C7AA9E96DDD9166BEC0EC81CEDB34186C70C5
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:39:54.020 17a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/05/04-17:39:54.082 17a0 Recovering log #3.2021/05/04-17:39:54.089 17a0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.234964548127225
Encrypted:	false
SSDEEP:	6:msO0q2Pwkn23iKKdKWT5g1IdqIFUtpdOL5vZZmwPdONcgFzkwOwkn23iKKdKWT5i:tO0vYf5Kkg5gSRFUtpdOdvZ/PdONLFzH
MD5:	8904230A04788CCFEB291012383A449C
SHA1:	05FB4FD9F0532B2FFFC3AC0A34B5F80DF11D5FB1
SHA-256:	D3863EB420E34B657EE460822F68C570F630C3033E866708955BD417A01E633E
SHA-512:	372D93F61EE28C85C947B237F13E8ECA17A67EEB0B2EFA3F9AFF4DD7D03023AAEADD780F83420131201B4FE1DF8F8B8E9DA8BBE849F02E66E6C272345FF8543
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:39:53.924 17a0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/05/04-17:39:53.931 17a0 Recovering log #3.2021/05/04-17:39:53.951 17a0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.08974069833325143
Encrypted:	false
SSDEEP:	6:l9bNFlqQCNa/lvoDO6fodBXMTvFhLoOo/lCxthijjqGCxC+/erA/:TL+A/0O6fodBcTLoNuQjjqGI/x/
MD5:	13D9F8F310B1FCC98B33FA9F7B7076DE
SHA1:	2C854A76770EE748251CAF1C2E0AF723B164FDAE
SHA-256:	E070347D9CEED8A27D930EF31AB27C7E1F9FC1C077ADDF8E766FA23CEAEAA759
SHA-512:	1C21075121CD3453D5ED118B328B8A2514048C2FC62B774A95A03D47DA511D62F604F06E0DEC24F06B90AB1FBF15601013B9A8F437D27CA269DF0766164C3BF3
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Size (bytes):	413
Entropy (8bit):	5.005047450525535
Encrypted:	false
SSDEEP:	12:qm19EtRGp8tn7ubvt3rBIE6VD+2OTWxjBk77sKk5E5v9:qxRZubN9IE6FnOCfY7sKjv9
MD5:	906DF6548FCE3E977A268229F951C2F4
SHA1:	81E73DF9A02F565EC04769321B4FCB18B490A5F9
SHA-256:	0E5B9B256DAF26E8B571276835F9B14DB48C6979C63FC2997DB0260CEAC1991F
SHA-512:	352AEA41B0CE55F586BB3DEAA3F9E2043C7DBA2CCE45796441A7B7CA8E0CEE86D758444D21F661074F4D67C6F83AD1BB3CE201068631049B5CE427938EACC7D4
Malicious:	false
Reputation:	low
Preview:	.....&....com..goldberglaws..https..onedrive*6.....com.....goldberglaws.....https.....onedrive..2.....a.....b.....c.....d.....e.....g.....h.....i.....l.....m.....n.....o.....p.....r.....s.....t.....v.....w...:&.....BI...E..... .....*.https://goldberglaws.com/2.Onedrive:.....J.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	33356
Entropy (8bit):	0.04761656801783401
Encrypted:	false
SSDEEP:	6:ysLTxB/idUwsfURxRg9bNFlWCj/lun/l3n:n/YkgqLBj/snt3n
MD5:	04B10E3FE436C2880290AB48E626894A
SHA1:	33D1796D9B0EA4A1732CD89C0646771363074AFC
SHA-256:	87F7499AD88514F219CDB777DF87DBFB43BC4727836F2F4AF39DD877651D396A
SHA-512:	96C2B7E8BCF5310781923071DE03518DD10544FF5EEDF691A5B6D5A8591A3DC03DEA2C2B01B2F730240623F0DD3FA245CF2BFE6DA329FBFF3D3C5E623D780B8
Malicious:	false
Reputation:	low
Preview:	.....\u..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.478172639703576
Encrypted:	false
SSDEEP:	48:AeG8E7C1a77My8dbZaqibQSefgGuNrS0U9RdiN9RE7F:dEWa77MxdbZaqibQ5fgGCrS03EZ
MD5:	241753D36F438B25A09955BC3AED5E6C
SHA1:	5F1EA0C39B8679C1B2E655AE497ECB08CD985F15
SHA-256:	F3B90DF06EE3F422D9FF30A2FDC1D9FCA80BA9CBB1C0E5F1810C810EADBF317D
SHA-512:	3C3E189C20743892FD49E7D33FD3BC21477E437E64FDB36B94E1A831DCC492CCA5BFCAC21C572D6CCD26832976F0480E9C10143822B34742C772D5ABD27B7E
Malicious:	false
Reputation:	low
Preview:	7sY...*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp .HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..225513000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-05-04 17:39:55.79][INFO][mr.Init] MR instance ID: 4d4c9811-bd73-4152-9fba-7c400adc997e\n","[2021-05-04 17:39:55.79][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-05-04 17:39:55.79][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-05-04 17:39:55.80][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-05-04 17:39:55.80][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-05-04 17:39:55.80][INFO][mr.CastProvider] Query enabled: true\n","[2021-05-04 17:39:55.80][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.206887332499012
Encrypted:	false
SSDEEP:	6:msH+q2Pwkn23iKKdK8a2jMGIFUtpdGmZmwPdGiVkwOwkn23iKKdK8a2jMmLJ:tH+vYf5Kk8EFUtpd9/PdBV5Jf5Kk8bJ
MD5:	A4446C55E3490AB55D1EF2E9CC466BD1
SHA1:	278845B3F7C96ACCB91B545E78AE787ED5D30FD4

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
SHA-256:	4F20A458AE8AFD00691CB94B30C649A6078809C6905EA1A327C80215D1FE367F
SHA-512:	D5042B98700763392319285FE5991B27192F61F0A128487A6EBB87D10ED9DD0C648070E8554FD651BF982D048034AE7F71E0CFA9D113450DF5F45AE06AE36D2B
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:39:44.133 159c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/05/04-17:39:44.135 159c Recovering log #3.2021/05/04-17:39:44.135 159c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.234804066330344
Encrypted:	false
SSDEEP:	6:msO9+q2Pwkn23iKKdKgXz4rRIFUtpdrJZmwPdKN9VkwOwkn23iKKdKgXz4q8LJ:tY+vYf5KkgXiuFUtpdd/PdWV5Jf5Kkgi
MD5:	D9B1CEB30947A919984B33AD85A0BA8E
SHA1:	3C427E3640D3B8E2BB27E9E6D15963CCDE121CD7
SHA-256:	08E41F80A54BE5C8F0CB554C47BF2F9E71E988E8897A2E81766D71A72DACA1A6
SHA-512:	CE9CF22C0B6B016208B108F1DB62C6717ED58994791598D82FBE4CFC300F26DE266CDB97D93B43662F00427B20D9898DFF1D2408D80C555BBF16CE043E505D5
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:39:44.445 152c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/05/04-17:39:44.446 152c Recovering log #3.2021/05/04-17:39:44.447 152c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	28672
Entropy (8bit):	1.2139517168547302
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUdT35ZmhbzLtph:wIElwQF8mpcSWb9o+bEYigP1
MD5:	ADED10F9F1B3B2593FC8ED5012DD1065
SHA1:	23DB2816AFA2D31A19D9968E06D95FB89527D149
SHA-256:	0C61AA86C35F36FAB3EE9AAC2CACD2AC1A87AF16CF731F223742069D84F0079C
SHA-512:	01F82565790579C68B5B65CDF29B48BA82DDCA20FF3DF4C2265068219865BBBDDE2633A78D256D2A27FE3B85A155171B332C4CC1D67B28C68A66A6A9F5A135E
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g...^.....j..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29252
Entropy (8bit):	0.6281633116254718
Encrypted:	false
SSDEEP:	48:Z8qkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUv4:Z8hIElwQF8mpcSU
MD5:	BABB0E1721E7E129A13DD948DD6A2C53
SHA1:	804B2273FCD567499F2135AF713C75A4EDA3E353
SHA-256:	B99FA30A86A2D4ED7FD98063DABB0B3F699ED042ADD18FD97D4CF0B46433E0BF
SHA-512:	BEF8535F8AE041E5D683370D200B57DE62DBDCE618B8AB1D081737F91DD1F88898BB951E8C2165CF7113B461396A88D3F9E46AE6607C1D0649DA312A4CF8005
Malicious:	false
Reputation:	low
Preview:	.....k..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl:5ljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.203621394690328
Encrypted:	false
SSDEEP:	6:msEK9+q2Pwkn23iKKdKrQMxIFUtpdqKJZmwPdqK9VkwOwkn23iKKdKrQMFLJ:tv+vYf5KkCFUtpdq0/PdqUV5Jf5KktJ
MD5:	AEA0BEDF5E8638E0A2EDC067335A7404
SHA1:	FC7014ACD63FA3DFFF820656989E1EC1A3A6D4ED
SHA-256:	4DA51A3CC65916C65D4290F8111CCF3E9A1654A6C166B90620A988855144D908
SHA-512:	FF273841906800DC4D591D9FCCA42A9CFEB833A099AB3247B8087423145AB0CF52E0D1404FB5EF574A8ED62BFC36F39C1A7B0BCA11E2616957A4D7279AF5D6F
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:39:44.354 152c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/05/04-17:39:44.356 152c Recovering log #3.2021/05/04-17:39:44.356 152c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.201667538321476
Encrypted:	false
SSDEEP:	6:msTdD+q2Pwkn23iKKdK7Uh2ghZIFUtpd9XZmwPddRGVkwOwkn23iKKdK7Uh2gnLJ:tTdavYf5KkIhHh2FUtpdZ/PddRW5Jf5m
MD5:	28CA647A1FF0CA29CFC202D94DFF64DF
SHA1:	9B6AEF4FDC918785A8E8AB1970320631611C3307
SHA-256:	3F3470086F84C5E549226CD6E7E77AEF29296796AF8C2E710968A69173B5C482
SHA-512:	DBB701739BF9D93F225602E712E7C6CD8F37BF1A9AB59C7E49D6A1A8FD3D1DAEF517239605BFD0BD37EE6913A0E552854F1F6F7C46C2DF38A3D17FFC4333B59
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:39:44.078 1438 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/05/04-17:39:44.085 1438 Recovering log #3.2021/05/04-17:39:44.088 1438 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\38bff282-14fe-4d23-a7e5-280bc3a6d216.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\38bff282-14fe-4d23-a7e5-280bc3a6d216.tmp	
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A5106422228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.266402680582677
Encrypted:	false
SSDEEP:	6:msYVq2Pwkn23iKKdKusNpV/2jMGIFUtpdC5gZmwPdC5IkwOwkn23iKKdKusNpV/s:tAvYf5KkFFUtpdr/Pdh5Jf5KkOJ
MD5:	6D2C06E34130FA4E7773D3BD789CACE8
SHA1:	E203F52089C79C7B60D30F241CF783004105D558
SHA-256:	DF75C75D90268A699C27E9923D81EA174FB4F66C1BF9B4771207DC003AE5B8D7
SHA-512:	47A59934840A5D09DAEEE9A8546C2166DD7217F0F1360D0C4498121614DE2089786675907E850D1DD629CD7A937C9D19FBE71D7B6A075A1D60C2C92EF8A521A
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:39:44.373 1434 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/05/04-17:39:44.375 1434 Recovering log #3.2021/05/04-17:39:44.375 1434 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.275237781679006
Encrypted:	false
SSDEEP:	12:tFrMvYf5KkmiuFUtpdry/Pdr+5Jf5Kkm2J:tJ2Yf5KkSgTrGroJf5Kkr
MD5:	1AB1AA1AEBD987036D0C9D193C33A785
SHA1:	36D3F42CFA366E899C31975D0485E1EE1B9C944D
SHA-256:	76AD4DF3C793F08D47911EDEAAB7BC17A96B1BFE7F5B2F30D03994C4B9D50847
SHA-512:	42E9A364A1BFF46901D64C1937BABA1C2530A72FFFA42E283DF6E96900278D0604F9A10EC0BDB1F581C0D686A6F8785E120F109B4D3E7485ECAE011C6A25614
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:39:44.429 1434 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/05/04-17:39:44.431 1434 Recovering log #3.2021/05/04-17:39:44.431 1434 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.196874314695424
Encrypted:	false
SSDEEP:	6:msw1VUuR6yq2Pwkn23iKKdKusNpZQMxIFUtpdw1VUK1ZmwPdw1VURRkwOwkn23iA:tGvYf5KkMFUtpdW1/Pdj5Jf5KkTJ
MD5:	F85B4B8A82D6F4A3569B3491E0415495
SHA1:	CCA899C525D5B298C8901BB662034923A9100450
SHA-256:	8E1584DFD046FFAB875CF9BB2DEAD4F4EA66E9F30CF0DB13164155D1086FA9CD
SHA-512:	83466436ECBCE442E4DAF2B8048425181E4F8AACFCF58F7DFB357CA526BAB694BA25956C2A88C53A5474FBC76C74435BDC6E5CFD36C371E1AB3CFB10DE1A0B0
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:40:01.240 1430 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/05/04-17:40:01.241 1430 Recovering log #3.2021/05/04-17:40:01.242 1430 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\97b4f9d4-bab1-4664-9472-59383c235807.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248516523181804","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Reputation:	low
Preview:	.'..(..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.2259287099142195
Encrypted:	false
SSDEEP:	12:tOOQvYf5KkkGHArBFUtpdOfW/PdOfq5Jf5KkkGHAryJ:tOOiYf5KkkGgPgTOqO8Jf5KkkGga
MD5:	E94ADFBC7BAB5ABB2158E87F1E7C141B
SHA1:	BC10053397C5298D5243D4124FB6FEA6C4C22031
SHA-256:	06E683494CBA59D24585174FB1EC12916583844DF74F8B9E3C5017FE9C1FEE5B
SHA-512:	3C701B9124544CF1114D3ABB84AEF56FC98FB691B320D4CD41B4F33666DB71798C53EA4B67E325A876E89E8F1FF519EB9E2C24C9E9E771C1597519F0F366A3C
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:39:53.270 1434 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/05/04-17:39:53.272 1434 Recovering log #3.2021/05/04-17:39:53.272 1434 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.293946454038712
Encrypted:	false
SSDEEP:	12:tOBFr4vYf5KkkGHArqiuFUtpdOD3J/PdOp3D5Jf5KkkGHArq2J:tOiYf5KkkGgCgTOLOplJf5KkkGg7
MD5:	A7381F5E1EC8DCE2EFB97E3FE3058E4A
SHA1:	16DA9C3EC02EF077EC6779BA728C34DFA845A624
SHA-256:	251837165D75CC182F65F159ACD44E09F9AE6A82EB7F8DB0B2E67D7D3FD26A89
SHA-512:	09246E0FEC5C3729AB027B62B4472A8403B42A12887992A2307ACB0DAE958EAD8BDA18ACCE0EC44EE0D48F31B5F747B67A4A0018158A59401B2078D3179D67C
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:39:53.282 17b8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2021/05/04-17:39:53.488 17b8 Recovering log #3.2021/05/04-17:39:53.491 17b8 Reusing old log C:\Users\user\ AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.176922036596957
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
SSDEEP:	12:tovYf5KkkGHArAFUtpd91/Pdd5Jf5KkkGHArfJ:taYf5KkkGgkgTFPJf5KkkGgV
MD5:	F109AA09FA39566B4AB20CA88AC9B2DA
SHA1:	BB8272BB8B23A8C13A971A0C97E12D537B998F31
SHA-256:	54B4B05F6281B4DE10A1B41873EE17B771C474C17465E366AABBC14D79CDA3D8
SHA-512:	12D95F8A98F06155BB88CC3119FC05E82F0CEF102308A9F83E770B8939A3BC59C01A66827BF81BA421588C326F1BDC83C388D89E8271B2C988ED853D1254FE11
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:40:08.830 1430 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/05/04-17:40:08.832 1430 Recovering log #3.2021/05/04-17:40:08.832 1430 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.2468285746849155
Encrypted:	false
SSDEEP:	6:ms1jyq2Pwkn23iKKdKpIFUtpd/1ZmwPddTXRkwOwkn23iKKdKa/WLJ:tgvYf5KkmFUtpd/1/PdRB5Jf5KkaUJ
MD5:	7B17525DF732AC48E51DD36CFA10E5C4
SHA1:	3999083B0FA9115F6FADFBF222B448F43A0C1726
SHA-256:	8B4AFCBC25F2C5D1E4883A5D1B2202D9B56764BE7363046176489DF9F7C28017
SHA-512:	3DF2081BFB69BE968B7540CFE5769FCEBDC7B7592B7151AECF1DC1BCA9FBEECED9D31F7FCF494D0FFDF952E30D01D5B5A7C58E5CDA81B88E0416D1EA31B4 564F
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:39:44.085 1430 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/05/04-17:39:44.089 1430 Recovering log #3.2021/05/04-17:39:44.096 1430 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.336884861378619
Encrypted:	false
SSDEEP:	12:tnxvYf5KkkOrsFUtpdr1/Pd75Jf5KkkOrzJ:t9Yf5Kk+gT3tJf5Kkn
MD5:	B5A6E40E9EB7F08F8100319EC48501FF
SHA1:	7C23B4D574CB816E754876CB683447224ACDEA52
SHA-256:	325F2EFF080A40D723549DD5751EB5A4473718872780A14C44020BFCA8F00D18
SHA-512:	A1EC3EDD26A3BAC25581D5343952CCED58BC5BA513F66A89CB2B3865CED8DAA8E8C3B0C0DA5747B114B0639FDE3ACE8FE8E6F6B5B25555011954311205 5CD 9E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Preview:	2021/05/04-17:39:55.783 1430 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/05/04-17:39:55.784 1430 Recovering log #3.2021/05/04-17:39:55.784 1430 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:B6:B6
MD5:	9135E6ADDAF7A86B99D634EFCFD0EE57
SHA1:	BA086F441C45BDB68EF28A788BCD9CBB4E4E6C2A
SHA-256:	01D9F417191B1DDC989EE7858C47AD4AF393387487BE92C2B8D29B18469ABAE4
SHA-512:	FEF357DF33CFDF204EB04DD1D6D31561CA63C1B51A8E676830DD321F3C17B981ECBDF99A33E13C7EF9AB1F3AE09BD0C05D06D0F3F7FDF753D3972ACE8DC6E46C
Malicious:	false
Reputation:	low
Preview:	....%....*._

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.52140275839823
Encrypted:	false
SSDEEP:	3:tUKDRIU38olFUSb2TyZmwv39RIU3/LVQSBbh7V8s9RIU3/LVQSBbh7WGv:msMolFHJZmwPdzSYbh7VvdzSYbh7tv
MD5:	D44F26963476BEEE04D1CFD34F56BB5F
SHA1:	D19FBCB1CAEFBE02BDFDD76A6B2ED900227341FC
SHA-256:	FEF830162B04F781361E72F51BBAB12E27FB43DB32EAE174249828B11A0E621D
SHA-512:	87C6F45B12BDD5268D3C7A94E61F398965AF17661B0C6F8C7E20D6E1CB89141A7972454C725A42507AEC9D359E572B467A63ACECE227CB1C200900A6F9E76A7
Malicious:	false
Reputation:	low
Preview:	2021/05/04-17:39:51.991 1724 Recovering log #3.2021/05/04-17:39:52.060 1724 Delete type=0 #3.2021/05/04-17:39:52.060 1724 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e9e8287e-aa15-4bc2-9df8-b7e6a9043739.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22602
Entropy (8bit):	5.536132994124018
Encrypted:	false
SSDEEP:	384:DNGt2LlgsXN1kXqKf/pUZNCgVLH2HfD/rUqqHGznZpywHj4m:nLlzN1kXqKf/pUZNCgVLH2Hf7rUzGzn/
MD5:	293352C28E97D73B30DEC453A2D5AF15
SHA1:	7A3FFDF0E44446163C09A1A11DEDABA1F7E946E4
SHA-256:	700AB0783ACBD7023542A64CA6D0A31DFCE416073EBFCCF82E4840C0A1E57303
SHA-512:	A4E1D1582BEA986EB988E127CEBC8DD79F302D53D719B0DD8FEBE21AA85F9141069FEBA21E25957725F83A171D1F47F25D7054180AA7A5B5A361FC2EA2FB043B
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13264616384083393","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fa0a058b-8415-4622-814b-b8396fcd01bc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19010
Entropy (8bit):	5.5671970671178865
Encrypted:	false
SSDEEP:	384:DNGt/LlgsXN1kXqKf/pUZNCgVLH2HfD/rUqqHGbyw2j4J:4LlzN1kXqKf/pUZNCgVLH2Hf7rUzG8jO
MD5:	7B11CCE817DC3BE888FBE45F9E5DE691
SHA1:	070F68FD2862BF97BBA14B1A2A29FEC8E78BB69C
SHA-256:	EFB68193B674A1181656B77F65C7ED40E77F8E84675A6553ED10FDE1B68A4CEE
SHA-512:	EC21A6472150FF56549D75BC2F6486F034AD912FABD14C2E654971BD2F2013F1C675D21E72099B534F72B16C0DFECD408D0C868E83A9BB7C2328277468E1D01(
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13264616384083393","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	335
Entropy (8bit):	5.262882887614389
Encrypted:	false
SSDEEP:	6:msl8+q2Pwkn23iKKdKfrzAdlFUtpdlwq5ZmwPdICNVkwOwkn23iKKdKfrzILJ:tCvYf5Kk9FUtpd6/Pdnz5Jf5Kk2J
MD5:	E922C78B52E400C26DE6F051EFB7DCF2
SHA1:	E1DDDAD2F7D4FEC694241F83A1F8E28BB0AD7D6A
SHA-256:	82525AD1EEED2A3BCB034DABFD1242F9918C49043081AE4E3AEF8138B81156AB
SHA-512:	20973F37F5D5D163D982B6422706CC4FB7B11E4E32EA80B0DDB11B85968C6DC12044EB90A6B8FD1346950E745E85F4BBFB42C19037F8E7859C69EAF6719E214F
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Reputation:	low
Preview:	2021/05/04-17:39:55.112 988 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/05/04-17:39:55.113 988 Recovering log #3.2021/05/04-17:39:55.114 988 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHlGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false
Reputation:	low
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\bea3ef04-1513-4261-8e94-a5cae7121e41.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	168434
Entropy (8bit):	6.0811015804926996
Encrypted:	false
SSDEEP:	3072:ItLi8A6zsByu8VXAVzkbOBLvMlNEopvR/XQrXaFcbXafIB0u1GOJmA3iuRG:GLT7OoQVzkq9vMwSR/LaqfllUOoSiuRG
MD5:	E4235F5C3D4B8A77474A902A8400832B
SHA1:	832B38EB20BD3AE17E49DBC9A4B48FE6E1F20B67
SHA-256:	3327A12FC11D6B69B372B72F5A473FDF3F9A150FAD40B8453AF917F177879508
SHA-512:	8198AE016CA01235CC3BBC6C2A919F2F98C04FFDD80D64B59830FCA2E03CB076AA06F35896315A499F39C9CD3C04E0E7FDFB6C3E070B59D554B54D2BAD1012E
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620142786669139e+12,"network":1.620142788e+12,"ticks":303096093.0,"uncertainty":3464151.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Temp\2aa01b41-85fd-4b42-b852-bae52ab28660.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)

C:\Users\user\AppData\Local\Temp\2aa01b41-85fd-4b42-b852-bae52ab28660.tmp	
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\9b4bd744-5b0b-4a06-b947-2bce36f5f741.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\browser-sslkeys.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	12960
Entropy (8bit):	4.64096862468895
Encrypted:	false
SSDEEP:	192:CU603A/YeX408HrovusL8uTPmw8rvUSsHg0MBLdYBLdjRLdwLdZBLdQ:Z603AAeI08HEvXL8uTPmw8wSsHgsW8
MD5:	3E21C707A53C5473D2269A467FCA94B4
SHA1:	D1692F546905EC49B11755310C08A47ED1B3C214
SHA-256:	7060032E3E3E0AEEEACFDAF44A8315A493A744C4518C86D791BE9ED712A22B12
SHA-512:	8066A05014B1DCBA95AD6A466D45BAF0BCD82D5EFC81EA667F6BD48EA3027623D1CC335E2910C047CE151C2F71C5D62B7AB4262B0C26305EDF1825B078E8818
Malicious:	false
Reputation:	low
Preview:	CLIENT_HANDSHAKE_TRAFFIC_SECRET 2af1f72cb00503f6e6b8f32ddc10e71d1dea42789d30bbc3668c1bd8c2f1e3a5 c2ca7fc7aba5559e7c77f27456387e932e5c42bd5c09cce0153cb0ffb9a5a309.SERVER_HANDSHAKE_TRAFFIC_SECRET 2af1f72cb00503f6e6b8f32ddc10e71d1dea42789d30bbc3668c1bd8c2f1e3a5 109728149bedfaee46be382dd6c8f83c43239ac687ee0e8bef459741d427361c.CLIENT_HANDSHAKE_TRAFFIC_SECRET d69ac932bf8c6485f97d71feec9e9eb3cfeffdabba17424251c819802c77cce9 0833fc878342249cf5079728b269ca4bdf6c58d6d9282a75b38cef055bfecdde.SERVER_HANDSHAKE_TRAFFIC_SECRET d69ac932bf8c6485f97d71feec9e9eb3cfeffdabba17424251c819802c77cce9 c8d8d161cca953cff59b4d0ec7c1ea15150968c3e6f1f61f6542856701d7a217.CLIENT_HANDSHAKE_TRAFFIC_SECRET b260331fd24a7c6ceca9e424254ce13a80c324a088a6f81a853be2bb58dc7a7d 64daa6f67bd1670cb49d078e68be7fb3759e7aedb9d34128cbac7358e5af5f04.SERVER_HANDSHAKE_TRAFFIC_SECRET b260331fd24a7c6ceca9e424254ce13a80c324a088a6f81a853be2bb58dc7a7d 1e3ecc28d9265b0094a9d4662ea96a59db1894a03a296c03d90ffad91b47c8c0.CLIENT_TRAFFIC_SECRET_0 d69a

C:\Users\user\AppData\Local\Temp\c2b5b53e-d865-4be6-8387-7f90b579614c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916

C:\Users\user\AppData\Local\Temp\c2b5b53e-d865-4be6-8387-7f90b579614c.tmp	
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v....;.._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&..._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.Ipr..Q....:... <.....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a..:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\d378f643-127b-4dee-ac81-0674b20b08f0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l.}.{...z...)y.n..'..).....,b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CEB4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\ca\messages.json	
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "C onnecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885B
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\es\messages.json	
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE018
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\es_419\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA3
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavailable": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BEAD8
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\fi\messages.json	
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavail able": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavai lable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOGAh
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.791154467711985
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOGAOf8SLm:Wh7qgYp1CMLUph1GiSLm
MD5:	E376D757C8FD66AC70A7D2D49760B94E
SHA1:	1525C5B1312D409604F097768503298EC440CC4D
SHA-256:	8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D
SHA-512:	673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA7555
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ... .".. },.. "app_name": {.. "message": "Chrome ... .".. },.. "craw_app_unavailable": {.. "messa ge": "..... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... ....".. },.. "iap_unavailable": {.. "message": "..-.. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome ... .".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\hr\messages.json	
Category:	dropped
Size (bytes):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D0 6E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw _app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comple ted.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyZnLAOfTYBIAYm:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYIAd
MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA 2
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "cr aw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be co mpleted.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD
MD5:	A328EEF5E841E0C72D3CD7366899C5C8

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\it\messages.json	
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_una vailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ....."... },.. "app_name": {.. "message": "Chrome ....."... },.. "craw_app_unavailable": {.. "message": "..... ....."... },.. "craw_connect_to_network": {.. "message": "....."... },.. "iap_unavailable": {.. "message": "....."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome ....."... }..}..

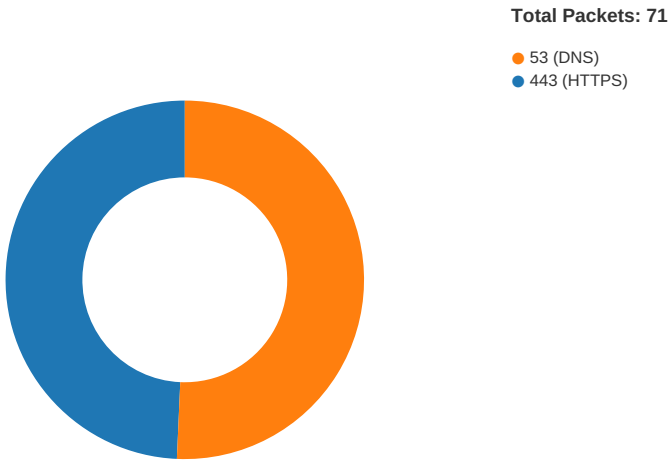
C:\Users\user\AppData\Local\Temp\scoped_dir4136_829614333\CRX_INSTALL_locales\ko\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	5.160315577642469
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyZnLAOfTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOGAOfyYA
MD5:	9F6B4D82A70C74CA751E2EAE70FAB5CF
SHA1:	0534F125FFCE8222277CF2BE3401C59DAF9217F8
SHA-256:	D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68
SHA-512:	ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome . ... .."... },.. "app_name": {.. "message": "Chrome . ... .."... },.. "craw_app_unavailable": {.. "message": ".. .. .."... },.. "craw_connect_to_network": {.. "message": "..... ....."... },.. "iap_unavailable": {.. "message": ".. .. .."... },.. "jwt_retrieve_failed": {.. " message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome. ....."... }..}..

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 17:39:47.509226084 CEST	49722	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:47.634243011 CEST	443	49722	40.76.138.32	192.168.2.4
May 4, 2021 17:39:47.634423018 CEST	49722	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:47.784025908 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:47.784720898 CEST	49722	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:47.907521963 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:47.907668114 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:47.916672945 CEST	443	49722	40.76.138.32	192.168.2.4
May 4, 2021 17:39:47.916708946 CEST	443	49722	40.76.138.32	192.168.2.4
May 4, 2021 17:39:47.916727066 CEST	443	49722	40.76.138.32	192.168.2.4
May 4, 2021 17:39:47.916917086 CEST	49722	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:47.951035976 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.082129002 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.082171917 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.082190037 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.082285881 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.427876949 CEST	49722	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.428889990 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.554698944 CEST	443	49722	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.554811001 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.557472944 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.600439072 CEST	49722	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.681277037 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.681317091 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.681337118 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.681356907 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.681377888 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.681443930 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.681488037 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.681510925 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.805788994 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.805824995 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.805847883 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.805870056 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.805890083 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.805902004 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.805910110 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.805931091 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.805938959 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.805949926 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.805965900 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.805983067 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.805999994 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.806005001 CEST	443	49725	40.76.138.32	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 17:39:48.806035995 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.883872032 CEST	49722	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.900432110 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.928998947 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929028988 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929047108 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929063082 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929079056 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929095030 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929102898 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.929110050 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929119110 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.929126978 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929141998 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929162025 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929177046 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.929181099 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929197073 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929204941 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.929214954 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929230928 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929246902 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929260015 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.929263115 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929279089 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929292917 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.929297924 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929316044 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929323912 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.929332018 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:48.929344893 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.929415941 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:48.948184967 CEST	49730	443	192.168.2.4	104.18.11.207
May 4, 2021 17:39:48.998878002 CEST	443	49730	104.18.11.207	192.168.2.4
May 4, 2021 17:39:48.998995066 CEST	49730	443	192.168.2.4	104.18.11.207
May 4, 2021 17:39:48.999227047 CEST	49730	443	192.168.2.4	104.18.11.207
May 4, 2021 17:39:49.009541988 CEST	443	49722	40.76.138.32	192.168.2.4
May 4, 2021 17:39:49.009563923 CEST	443	49722	40.76.138.32	192.168.2.4
May 4, 2021 17:39:49.009668112 CEST	49722	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:49.024179935 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:49.024207115 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:49.024298906 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:49.049859047 CEST	443	49730	104.18.11.207	192.168.2.4
May 4, 2021 17:39:49.053157091 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:49.053189039 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:49.053214073 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:49.053236961 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:49.053263903 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:49.053286076 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:49.053297043 CEST	49725	443	192.168.2.4	40.76.138.32
May 4, 2021 17:39:49.053308964 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:49.053332090 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:49.053354979 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:49.053380966 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:49.053426027 CEST	443	49725	40.76.138.32	192.168.2.4
May 4, 2021 17:39:49.053448915 CEST	443	49725	40.76.138.32	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 17:39:38.232084036 CEST	59920	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:38.291721106 CEST	53	59920	8.8.8.8	192.168.2.4
May 4, 2021 17:39:39.037354946 CEST	57458	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:39.097548008 CEST	53	57458	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 17:39:39.838901043 CEST	50579	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:39.899328947 CEST	53	50579	8.8.8.8	192.168.2.4
May 4, 2021 17:39:40.615752935 CEST	51703	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:40.668822050 CEST	53	51703	8.8.8.8	192.168.2.4
May 4, 2021 17:39:41.469403982 CEST	65248	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:41.518954992 CEST	53	65248	8.8.8.8	192.168.2.4
May 4, 2021 17:39:42.360354900 CEST	53723	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:42.410244942 CEST	53	53723	8.8.8.8	192.168.2.4
May 4, 2021 17:39:43.280374050 CEST	64646	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:43.330063105 CEST	53	64646	8.8.8.8	192.168.2.4
May 4, 2021 17:39:47.421185970 CEST	49714	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:47.444211006 CEST	58028	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:47.447966099 CEST	53097	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:47.451874018 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:47.486143112 CEST	53	49714	8.8.8.8	192.168.2.4
May 4, 2021 17:39:47.501461983 CEST	53	58028	8.8.8.8	192.168.2.4
May 4, 2021 17:39:47.512738943 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 17:39:47.516767979 CEST	53	49257	8.8.8.8	192.168.2.4
May 4, 2021 17:39:48.734203100 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:48.793625116 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 17:39:48.878314972 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:48.878367901 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:48.879813910 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:48.880261898 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:48.884866953 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:48.929694891 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 17:39:48.937104940 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 17:39:48.945219040 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 17:39:48.945435047 CEST	53	63153	8.8.8.8	192.168.2.4
May 4, 2021 17:39:48.947180986 CEST	53700	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:48.949381113 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 17:39:49.004695892 CEST	53	53700	8.8.8.8	192.168.2.4
May 4, 2021 17:39:49.011786938 CEST	51726	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:49.063163996 CEST	53	51726	8.8.8.8	192.168.2.4
May 4, 2021 17:39:49.268768072 CEST	56794	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:49.315684080 CEST	56534	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:49.316023111 CEST	56627	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:49.317367077 CEST	53	56794	8.8.8.8	192.168.2.4
May 4, 2021 17:39:49.364419937 CEST	53	56534	8.8.8.8	192.168.2.4
May 4, 2021 17:39:49.385533094 CEST	53	56627	8.8.8.8	192.168.2.4
May 4, 2021 17:39:50.039021015 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:50.087869883 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 17:39:50.213339090 CEST	63116	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:50.275666952 CEST	53	63116	8.8.8.8	192.168.2.4
May 4, 2021 17:39:50.566984892 CEST	64078	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:50.610575914 CEST	64801	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:50.623897076 CEST	53	64078	8.8.8.8	192.168.2.4
May 4, 2021 17:39:50.676115990 CEST	53	64801	8.8.8.8	192.168.2.4
May 4, 2021 17:39:50.955950022 CEST	61721	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:51.004641056 CEST	53	61721	8.8.8.8	192.168.2.4
May 4, 2021 17:39:52.415040016 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:52.472137928 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 17:39:52.818028927 CEST	49612	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:52.866585970 CEST	53	49612	8.8.8.8	192.168.2.4
May 4, 2021 17:39:53.485059977 CEST	49285	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:53.558386087 CEST	53	49285	8.8.8.8	192.168.2.4
May 4, 2021 17:39:56.374438047 CEST	59172	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:56.431854963 CEST	53	59172	8.8.8.8	192.168.2.4
May 4, 2021 17:39:56.772578955 CEST	62420	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:56.822185040 CEST	53	62420	8.8.8.8	192.168.2.4
May 4, 2021 17:39:57.755983114 CEST	60579	53	192.168.2.4	8.8.8.8
May 4, 2021 17:39:57.807317019 CEST	53	60579	8.8.8.8	192.168.2.4
May 4, 2021 17:40:03.600013018 CEST	50183	53	192.168.2.4	8.8.8.8
May 4, 2021 17:40:03.651576996 CEST	53	50183	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 17:40:04.611169100 CEST	61531	53	192.168.2.4	8.8.8.8
May 4, 2021 17:40:04.661916018 CEST	53	61531	8.8.8.8	192.168.2.4
May 4, 2021 17:40:32.754303932 CEST	49228	53	192.168.2.4	8.8.8.8
May 4, 2021 17:40:32.811599970 CEST	53	49228	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 17:39:47.444211006 CEST	192.168.2.4	8.8.8.8	0xfe20	Standard query (0)	goldbergla ws.com	A (IP address)	IN (0x0001)
May 4, 2021 17:39:48.878314972 CEST	192.168.2.4	8.8.8.8	0x5ba2	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
May 4, 2021 17:39:48.878367901 CEST	192.168.2.4	8.8.8.8	0xd732	Standard query (0)	maxcdn.boo tstrapcdn.com	A (IP address)	IN (0x0001)
May 4, 2021 17:39:48.884866953 CEST	192.168.2.4	8.8.8.8	0xd094	Standard query (0)	kit.fontaw esome.com	A (IP address)	IN (0x0001)
May 4, 2021 17:39:49.316023111 CEST	192.168.2.4	8.8.8.8	0x1dd3	Standard query (0)	cdnjs.clou dflare.com	A (IP address)	IN (0x0001)
May 4, 2021 17:39:50.213339090 CEST	192.168.2.4	8.8.8.8	0xa221	Standard query (0)	ka-f.fonta wesome.com	A (IP address)	IN (0x0001)
May 4, 2021 17:39:50.610575914 CEST	192.168.2.4	8.8.8.8	0x9edf	Standard query (0)	blobs.offi cehome.mso cdn.com	A (IP address)	IN (0x0001)
May 4, 2021 17:39:52.415040016 CEST	192.168.2.4	8.8.8.8	0xf948	Standard query (0)	blobs.offi cehome.mso cdn.com	A (IP address)	IN (0x0001)
May 4, 2021 17:39:53.485059977 CEST	192.168.2.4	8.8.8.8	0xf4ad	Standard query (0)	clients2.g oogleuserc ontent.com	A (IP address)	IN (0x0001)

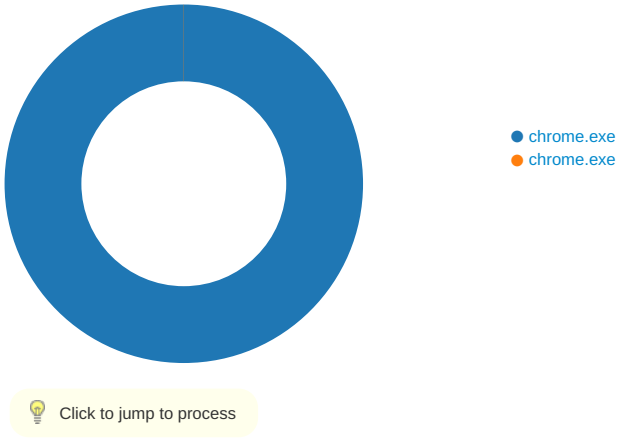
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 17:39:47.501461983 CEST	8.8.8.8	192.168.2.4	0xfe20	No error (0)	goldbergla ws.com		40.76.138.32	A (IP address)	IN (0x0001)
May 4, 2021 17:39:48.929694891 CEST	8.8.8.8	192.168.2.4	0x5ba2	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 17:39:48.945219040 CEST	8.8.8.8	192.168.2.4	0xd732	No error (0)	maxcdn.boo tstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
May 4, 2021 17:39:48.945219040 CEST	8.8.8.8	192.168.2.4	0xd732	No error (0)	maxcdn.boo tstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
May 4, 2021 17:39:48.949381113 CEST	8.8.8.8	192.168.2.4	0xd094	No error (0)	kit.fontaw esome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 17:39:49.385533094 CEST	8.8.8.8	192.168.2.4	0x1dd3	No error (0)	cdnjs.clou dflare.com		104.16.19.94	A (IP address)	IN (0x0001)
May 4, 2021 17:39:49.385533094 CEST	8.8.8.8	192.168.2.4	0x1dd3	No error (0)	cdnjs.clou dflare.com		104.16.18.94	A (IP address)	IN (0x0001)
May 4, 2021 17:39:50.275666952 CEST	8.8.8.8	192.168.2.4	0xa221	No error (0)	ka-f.fonta wesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 17:39:50.676115990 CEST	8.8.8.8	192.168.2.4	0x9edf	No error (0)	blobs.offi cehome.mso cdn.com	wildcard.officehome.msocdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 17:39:52.472137928 CEST	8.8.8.8	192.168.2.4	0xf948	No error (0)	blobs.offi cehome.mso cdn.com	wildcard.officehome.msocdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 17:39:53.558386087 CEST	8.8.8.8	192.168.2.4	0xf4ad	No error (0)	clients2.g oogleuserc ontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 17:39:53.558386087 CEST	8.8.8.8	192.168.2.4	0xf4ad	No error (0)	googlehost ed.l.googl euserconte nt.com		216.58.212.129	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 4136 Parent PID: 5112

General

Start time:	17:39:43
Start date:	04/05/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://goldberglaws.com/'
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF609CBFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: 4676 Parent PID: 4136

General

Start time:	17:39:44
Start date:	04/05/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1572,3517170012200295616,8387480202046539603,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1812 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly